![CLOUDFLARE]

Data Loss Prevention

Protect sensitive data and ensure regulatory compliance across web, private, SaaS, cloud, AI, and email apps.

The most integrated data loss prevention (DLP) for the agentic era

With Cloudflare DLP, you can detect and block sensitive data exfiltration across your network and applications (SaaS, AI, cloud, private, and email) without disrupting or slowing down user productivity.

Protect your intellectual property, source code, customer PII, and other data to:

- **Enforce compliance** using pre-built profiles for financial data, medical records, and social security numbers.

- **Safeguard corporate data** by blocking sensitive uploads to unauthorized cloud storage or file-sharing sites.

- **Secure AI prompts** by scanning and redacting sensitive data or source code in inputs to tools like ChatGPT and GitHub.

- **Gain visibility into data movement** across your entire hybrid workforce.

Built on Cloudflare's global edge, inspection occurs milliseconds from the user, ensuring fast and cost-efficient protection at scale.

Infrastructure provider

Identified SaaS vulnerabilities — like sensitive SharePoint files being widely shared — to help mitigate data loss.

[Read case study](#)

Leading digital bank

Consolidated security into a single dashboard, ensuring strict data compliance and ransomware protection for their mobile-first banking platform.

Telehealth provider

Secured sensitive patient data (PHI/HIPAA) and accelerated access for a rapidly growing remote workforce using DLP and CASB.

The Cloudflare difference

Simplified SaaS & AI security

Govern workforce AI usage by blocking suspicious content, and reduce exfiltration risks by identifying and remediating sensitive data stored across SaaS and cloud environments.
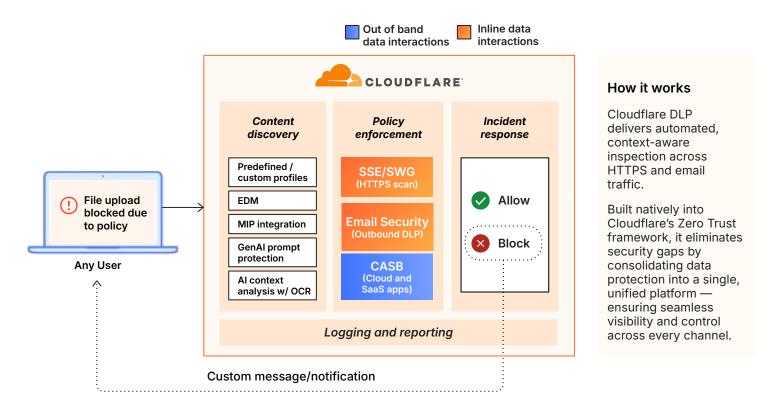
Unified policy management

Configure DLP profiles, detection entries, and Microsoft Purview sensitivity labels to consolidate protections across outbound traffic, documents, PDFs, and images.

Adaptive data controls

Give feedback per detection to refine AI context analysis and improve detection accuracy. DLP adapts to your specific data patterns and traffic to reduce false positives.

Want to go deeper on this product? Review our [reference architecture](#) or [talk to an expert.](#)

Data protection across all workspace channels

How it works

Cloudflare DLP delivers automated, context-aware inspection across HTTPS and email traffic.

Built natively into Cloudflare's Zero Trust framework, it eliminates security gaps by consolidating data protection into a single, unified platform — ensuring seamless visibility and control across every channel.

Sample DLP capabilities	
DLP profiles	Deploy predefined profiles for PII, PHI, financial data, and credentials, or build custom profiles to secure proprietary assets like internal project names or unreleased intellectual property.
Microsoft Information Protection (MIP)	Ingest MIP sensitivity labels to automatically enforce policies (e.g., Block "Confidential") without re-tagging files.
Exact Data Match (EDM)	Upload hashed datasets (e.g., a specific customer database) to detect exact values rather than generic patterns. Block specific records while drastically reducing false positives.
Document fingerprinting	Secure sensitive documents by creating and storing unique "fingerprints" (hashes/patterns) that are then compared with network traffic to identify and block similar documents.
GenAI prompt protection	Prevent sensitive data (source code, customer PII) from being pasted into public LLMs. Inspect HTTPS requests to tools like ChatGPT or Gemini to enforce safe AI usage.
AI context analysis & confidence scoring	Use machine learning to analyze context and proximity keywords. Set confidence thresholds to automatically block high-risk matches while logging lower-confidence events for tuning.
Optical Character Recognition (OCR)	Automatically scan and extract text from image files (PNG, JPG/JPEG) to prevent users from bypassing security by screenshotting sensitive documents.
User coaching and education	Display customizable, real-time notifications that instantly educate users on security policy violations.
Unified forensics and logging	Combine granular event logging with secure payload inspection. Analyze specific data snippets and user context to instantly validate incidents and fine-tune policies.